用户需求书

一、活动需求书

序号	名称	参考规格及技术参数	数量	单位
一	网络布线设备			
1	路由器	1*GEWAN,1*GEcomboWAN,1*10GEFP+,8*GE LAN,2*USB,2*SIC	1	台
2	汇聚交换机	24 个 10/100/1000BASE-T 以太网端口,4 个千兆 SFP,含 1 个 60W 交流电源	1	台
3	光模块	光模块-eSFP-GE-单模模块(1310nm,10km,LC)	12	个
4	接入交换机	24 个 10/100/1000BASE-T 以太网端口,4 个千兆 SFP,交流供电	6	台
5	壁挂式机柜	6U 高度，尺寸约（宽）550×（深）400×（高）350mm	6	个
6	服务器机柜	42U 高度，尺寸约（宽）600×（深）800×（高）2045mm	1	个
7	信息模块	五类信息模块	25	个
8	水晶头	五类线	2	包
9	光纤配线架	8 口	6	个
10	光纤	12 芯	560	米
11	光纤跳线	3 米	12	条
12	电源线	RVV2*2.5	560	米
13	楼层配电箱	定做国标	6	个
14	机房总配电箱	定做国标	1	个
15	线管	Φ20	650	米
二	安全设备			
1	综合日志审计	1、标准 1U 硬件，1 个 console 口，1 管理口，网口类型：1000M 电口*4，硬盘：1T，内存：8G，单电源，CF 卡启动，日志处理能力 200EPS。资产授权：15 个。提供 3 年设备原厂保修服务。	1	台

		2、能对网络设备、安全设备和系统、主机操作系统、数据库以及各种应用系统的日志、事件、告警等安全信息进行全面的审计； 3、▲可以对选中的日志进行事件拓扑分析，并可视化的展示一幅描述日志之间的行为相关关系的事件拓扑图；（要求提供功能截图证明，并加盖厂家公章或投标专用章） 4、系统具有日志关联分析的能力，能够对不同的日志进行相关性分析，发掘潜在的信息； 5、▲告警内容可以自定义，可以根据日志的实际情况将参数（即预定义变量）传递给命令行脚本；（要求提供功能截图证明，并加盖厂家公章或投标专用章） 6、▲具备告警抑制功能，可以把同一时间内相同的告警合并成一条事件进行展示，告警抑制规则中的时间范围与合并数目可以手动进行配置，告警抑制规则可实时启用和停用；（要求提供功能截图证明，并加盖厂家公章或投标专用章） 7、▲系统应提供日志维护功能，能够自动定时备份采集上来的安全事件（日志），也支持手动备份与恢复。（要求提供功能截图证明，并加盖厂家公章或投标专用章） 8、需提供厂家针对本项目的授权书。 9、产品须获得中华人民共和国公安部的《计算机信息系统安全专用产品销售许可证》（三级）（要求提供复印件并加盖厂家公章或投标专用章） 10、所投网络安全产品厂家需具备《中国国家信息安全漏洞库（CNNVD）技术支撑单位一级》资质（要求提供复印件并加盖厂家资产授权：		
2	安全网关	1、标准 1U 硬件平台，单交流电源；含 6*GE 电口，2 个 USB 接口，1 个 RJ45 串口；网络吞吐性能 4Gbps；最大并发连接数大于 150 万,每秒新建 HTTP 连接数大于 4 万。下一代防火墙模块，基本网络防火墙功能，IPSEC VPN 功能，攻击防护，访问控制功能，用户认证功能，链路负载均衡功能、流量控制功能。 2、支持上网行为管理许可（APP&URL），关键字过滤和基于超过 2000 万域名的 URL 数据库可以帮助管理员轻松设置禁止访问的网页，控制对不良网站的访问。 3、支持防病毒许可（AV），支持大病毒文件的扫描，实时病毒连接阻断，病毒事件记录，支持常见病毒传输协议 HTTP、FTP 及各种邮件协议扫描。 4、支持入侵检测与防御许可（IPS），基于状态、精准的高性能攻击检测和防御，实时攻击源阻断、IP 屏蔽、攻击事件记录，支持针对多种协议和应用的攻击检测和	1	台

		防御，支持 SQL 注入和 XSS 防御、外链防护和 Web 访问控制。 5、▲必须支持基于 WEB 地址 URL 的策略路由，可实现将不同类型的网站流量智能分配到不同的链路。（要求提供功能截图证明，并加盖厂家公章或投标专用章） 6、必须支持 IP/MAC 地址绑定的方式防止 ARP 欺骗，可采用手动建立或自动探测的方式生成 IP/MAC 对。 7、支持一体化安全策略配置，可以通过一条策略实现用户认证、IPS、AV、URL 过滤、协议控制、流量控制、并发限制、新建限制、垃圾邮件过滤、审计等功能,简化用户管理。（要求提供功能截图证明，并加盖厂家公章或投标专用章） 8、▲支持基于策略的入侵检测与防护，可针对不同的源目 IP 地址、源 MAC 地址、服务、时间、安全域、用户等，采用不同的入侵防护策略。（要求提供功能截图证明，并加盖厂家公章或投标专用章） 9、需提供厂家针对本项目的授权书。 10、产品具有中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》（要求提供复印件并加盖厂家公章或投标专用章） 11、产品具有中国国家信息安全测评认证中心颁发的《信息技术产品安全测评证书》（EAL4+）（要求提供复印件并加盖厂家公章或投标专用章）。 12、产品具备中华人民共和国工业和信息部颁发的《电信设备进网许可证》（要求提供复印件并加盖厂家公章或投标专用章） 13、所投网络安全产品厂家需获得中国信息安全测评中心颁发的:《信息安全服务资质证书-安全工程类(三级)》（要求提供复印件并加盖厂家公章或投标专用章）		
3	运维审计与风险控制系统	1、标准 1U 硬件，含 2*GE 电管理口，4*GE 电业务口,硬盘:1T，1*RJ45 串口，单电源。最大资产数 100 个，最大字符连接 700 个，最大图型连接 200 个。 2、支持 NAT 地址映射部署，通过映射后的 IP 地址访问堡垒机进行管理和运维操作； 3、支持对运维操作（telnet/ssh/ftp/sftp/RDP/VNC/X11)的集中管理、访问控制、单点登录以及操作审计等功能； 4、▲支持不同的资源使用相同的 IP 或域名，便于同一资源按照不同的服务类型进行分类管理；（要求提供功能截图证明，并加盖厂家公章或投标专用章） 5、▲支持 RDP、VNC 图形操作过程中键盘输入操作记录	1	台

		和鼠标点击行为记录，并支持开启或关闭键盘输入审计功能；（要求提供功能截图证明，并加盖厂家公章或投标专用章） 6、支持 web 页面防跳转功能，进行 http/https 访问过程中，运维人员仅允许访问授权地址（要求提供功能截图证明，并加盖厂家公章或投标专用章） 7、支持 WEB 在线视频回放方式重现维护人员对服务器的所有操作过程。 8、需提供厂家针对本项目的授权书。 9、产品具备公安部《计算机信息系统安全专用产品销售许可证》-运维安全管理-增强级（要求提供复印件并加盖厂家公章或投标专用章）。 10、所投网络安全产品厂家需具备《网络安全应急服务支撑单位-国家级》（要求提供复印件并加盖厂家公章或投标专用章）		
4	WEB 应用防火墙	1、标准 1U 硬件，含 2*GE 电管理口，4*GE 电业务口（含 2 组硬件 BYPASS 模块），1*RJ45 串口，单电源。吞吐量:1Gbps,HTTP 最大并发数:5 万,HTTP 新建连接(CPS)：5000，物理保护链路 4 路，保护站点无限制，提供 3 年设备原厂保修服务，3 年 Web 应用防护特征库。 2、应具备 Web 恶意扫描防护的检测与防御能力，专利级别防护能力 （要求提供功能截图证明，并加盖厂家公章或投标专用章）。 3、支持对 Web 相关应用协议进行自定义，并提供详细协议分析变量。 4、▲具备业务合规功能，可对业务进行恶意试探、恶意撞库、恶意登录等行为进行检测及拦截（要求提供功能截图证明，并加盖厂家公章或投标专用章）。 5、具备网站锁功能，对网站进行锁定，可按日期、周期进行锁定时间设置 6、▲应支持和 APT 进行动态联动，满足用户对 Web 应用安全防护和 APT 联动需求。（要求提供功能截图证明，并加盖厂家公章或投标专用章） 7、具备多设备拓扑显示功能，可以在界面上以图形化的方式显示当前的部署拓扑。（要求提供功能截图证明，并加盖厂家公章或投标专用章） 8、具备 Web 安全事件的报表功能，支持一般的单一条件报表输出、专业的多维度统计报表输出。 9、需提供厂家针对本项目的授权书。 10、产品具备公安部《计算机信息系统安全专用产品销售许可证》（增强级）（要求提供复印件并加盖厂家公	1	台

		章或投标专用章）。 11、▲产品获得《网络关键设备和网络安全专用产品安全认证》（增强级）（要求提供复印件并加盖厂家公章或投标专用章）。 12、所投网络安全产品厂家需具备《网络安全应急服务支撑单位-国家级》（要求提供复印件并加盖厂家公章或投标专用章）		
5	APT 攻击防护	1、硬件外形：软硬一体化 2U 标准机架式设备；电源：1+1 冗余电源，CPU：4 核 4 线程*1，内存：16G，硬盘容量：2T*1，接口数量：标配 6 个，接口类型：千兆 RJ45 网口*2(管理口*2)、千兆 RJ45 网口*4，接口扩展：千兆 SFP 光口*4，MTBF 大于 65000 小时，吞吐率：网络层：1Gbps，应用层：500Mbps，WEB 检测：HTTP 最大并发数 7 万/秒，邮件检测：邮件处理数：100 万封/24 小时，文件检测：3 万个/24 小时，支持管理节点 10 个。提供 3 年设备原厂保修服务。 2、具备 110 种以上格式的文件检测能力，涵盖 Windows、Linux、Android 等多种操作系统，支持自定义文件类型。 3、▲需具备不少于 3 种检测机制（静态检测、漏洞检测、行为检测），每种检测机制检测流程可自定义配置。（要求提供功能截图证明，并加盖厂家公章或投标专用章） 4、▲支持不少于 10 种样本检测工作流配置，每种工作流可自定义选取相应的样本格式。（要求提供功能截图证明，并加盖厂家公章或投标专用章） 5、具备邮件检测、HTTP 检测、FTP 检测、SMB 检测，支持可疑样本手动上传检测。 6、▲具备事件特征库不少于 5000 条以上，并且可以按照协议类型、攻击类型、安全类型、流行程度、事件级别等分类编排事件特征。（要求提供功能截图证明，并加盖厂家公章或投标专用章） 7、具备弱口令检测，口令配置项不少于 7 种。 8、具备邮件报警能力，将报警信息通过邮件发送给管理员。 9、▲支持通过 Kafka 接口将样本检测日志、特征检测日志、隐蔽信道日志、恶意 URL 日志发送给第三方平台。（要求提供功能截图证明，并加盖厂家公章或投标专用章） 10、需提供厂家针对本项目的授权书。 11、具备公安部《计算机信息系统安全专用产品销售许可证》-安全监测产品-增强级（要求提供复印件并加盖厂家公章或投标专用章） 12、所投网络安全产品厂家需获得国家信息安全认证中	1	台

		心颁发的《信息安全风险评估服务一级资质认证》（要求提供复印件并加盖厂家公章或投标专用章）		
三	系统集成费		1	项

二、其他要求

1. 建设工期：合同签订生效之日起 30 天内。如有变更，最终按照业主要求的具体时间来执行。

2. 建设地点：用户指定地点。

3. 付款条件：采购双方签订合同时另行约定。

4. 验收要求：按用户要求进行验收。